ネットワーク技術の修得

第三技術室システム設計技術班　　篠　競

1　はじめに

現在、WWW などによって注目を集めている Internet の基礎となっているのが TCP/IP プロトコルである。

日常の業務でもこの Internet に接続された計算機環境を利用している。しかし、ネットワーク技術についての知識は業務に必要な断片的なものでありネットワーク技術、とくに TCP/IP プロトコルの詳細について理解しているわけではない。ネットワーク技術が急速に発展している今、TCP/IP プロトコルについての系統だった知識の修得は将来の業務の遂行のためにも有益である。

そこで今回、「TCP/IP によるネットワーク構築 Vol. II」、「TCP/IP によるネットワーク構築 Vol. III」、「NIS+ & DNS アドミニストレーションガイド」の 3 冊の図書を使用して、TCP/IP プロトコルに関するネットワーク技術を研修した。

研修に利用した図書の内容について簡単に説明する。「TCP/IP によるネットワーク構築 Vol. II」は、Xinu オペレーティングシステムへの実装を例として TCP/IP プロトコルを考察している。「TCP/IP によるネットワーク構築 Vol. III」では、TCP/IP プロトコルを利用して分散アプリケーションをどのように設計し構築するか記述している。「NIS+ & DNS アドミニストレーションガイド」は、システムとネットワークの管理者がどのように NIS+を設定、管理すればよいか、について書かれている。

TCP/IP は複数のプロトコル (通信手順) の集合であり、そこに含まれている技術は複雑でまた多様である。また今回の研修だけで TCP/IP プロトコルを理解できたわけでもないので、ここでは Internet と TCP/IP プロトコルについて基本的な部分である、ARP、TCP/IP、IP、ICMP、UDP、TCP などについて研修の成果として報告する。

2　インターネットと IP アドレス

Internet は、物理的にいえば世界中に分散して存在する複数のネットワークがゲートウェイを介して相互に接続されたネットワーク集合体である。しかし、Internet のユーザから見ると Internet は世界中に広がる巨大ではあるが単一のネットワークである。Internet のユーザは Internet にある資源をユーザ自身のホスト (計算機) の資源と同じように容易に利用できる。世界的な規模の複雑な物理的ネットワーク集合の存在を隠してユーザには Internet という仮想的なひとつのネットワークを提供するための基盤となる技術が TCP/IP プロトコルである。

Internet に接続する各ホストを一意に識別するために使われているのが IP アドレスである。IP アドレスは 4 バイト長で、普通 1 バイトごとに '.' で区切った 10 進数で表す。福井大学を例とすると、IP アドレスは 133.7.51.1 のように記述される。最初の 2 バイトが福井大学のネットワークを指定し、後半の

2バイトで各ホストを指定するようになっている。IP アドレスがネットワーク部とホスト部の2つの部分で構成されていることは、経路制御などを効率的に行なえるという利点の反面、物理的なネットワークへの依存を残すという欠点を持っている。

3 TCP/IP Internet の概念的階層

複雑な問題を複数の部分に分割して処理することは一般的方法である。ネットワークの構築ではプロトコルを階層化することで複数のプロトコルに分割し、各プロトコルの作成を容易にしている。またプロトコルを階層化、抽象化することで階層間のインターフェース部を明確にすることができ、各プロトコルについての研究や開発が容易になる。TCP/IP ソフトウエアは 4 つの概念層から構成されており、それらは5番目の層であるハードウェアの上に構築されている。

アプリケーション層 telnet、ftp、NFS、NIS などのアプリケーションプログラム

トランスポート層 TCP、UDP など。この層から下は普通オペレーティングシステムに実装

インターネット層 IP、ICMP。この層から上では、IP アドレスのみが使用されている

ネットワーク・インターフェース層 ARP など

ハードウェア層 ethernet、FDDI など

以下では、これらの層に対応するプロトコルに付いて説明していく。

4 ARP

物理ネットワークの中で IP アドレスからイーサネットなどの物理アドレスへの対応づけを行なうプロトコルである。Internet の IP アドレスは物理アドレスに依存していないため IP データグラムの転送に先立ってこの対応づけを必要とする。

物理ネットワークのパケットに解決したい IP アドレスを含んだ ARP メッセージを入れてブロードキャストし、対応する IP アドレスを持ったホストはこれに応答する。各ホストはこうしたやり取りによって IP アドレスと物理アドレスの対応をキャッシュする。このほかに、物理アドレスから IP アドレスを対応づけるプロトコルとして RARP がある。

5 IP と ICMP

Internet を IP アドレスに基づいたひとつの仮想ネットワークにみせているのが IP である。IP プロトコルは信頼性のない、コネクションレスのサービスを提供する。IP を定義づけるものとして次の3点を指摘できる。

- TCP/IP インターネットを通して用いられるデータ転送の基本単位
- 経路制御の機能を実行
- 上記以外の信頼性のない配送のアイディアを具体化する規則集合

Internet では基本転送単位を IP データグラムと呼ぶ。Internet に含まれる物理ネットワークやゲートウェイを通過して目的地まで配送されるものが IP データグラムである。これは、ヘッダとデータで構成されている。ヘッダ部分には自分と相手の IP アドレスのほかさまざまな情報が入っている。IP データグラムの配送で重要な概念としてフラグメント化、生存時間などがある。

IP データグラムは必ず終点に配送されるとは保証されていない。配送の途中で失われるかも知れない。このために信頼性がないといわれる。IP では IP データグラム単位で配送を行なうだけであり、IP データグラム間の関係を考慮しない。このため目的地では配送経路の問題で IP データグラムの順番が入れ替わって受け取られてしまうかも知れない。これをコネクションレスという言葉で表現している。

Internet は複数のネットワークがゲートウェイを通して結合したものだと説明した。ネットワーク間の結合はひとつのゲートウェイによるとは限らない。実際、複数のゲートウェイによって接続されていることのほうが普通であり、そのため目的のホストへの経路は複数ありうる。また、接続の変更や障害などによりネットワークの経路が常に安定しているとは限らない。ここに、配送のために最適な経路を選択する経路制御の必要性がある。

IP が実行する経路制御は 2 つの形式に分けることができ、それは直接経路制御と間接経路制御である。直接経路制御は、同一の物理ネットワーク内でのデータグラムの転送で、ゲートウェイを通らないものである。前述の ARP により IP アドレスと物理アドレスとの対応をとりデータグラムを配送する。

ゲートウェイを越えてデータグラムを転送する間接経路制御で主要な役割を果たすのはゲートウェイである。あるホストから Internet 上の目的のホストにデータグラムを転送する場合、相手のホストが同じ物理ネットワークにない時、ホストはゲートウェイにデータグラムを送る。データグラムを受け取ったゲートウェイはデータグラムの目的地への経路を判断して次のゲートウェイにデータグラムを転送する。この繰り返しで直接データグラムを配送できるゲートウェイまで転送され、目的のホストへは直接経路制御で転送される。

一般的に使用される間接経路制御の方式はテーブル駆動式 IP 経路制御といわれるもので、Internet 経路制御テーブルを利用して経路を決めるものである。このテーブルは個々のホストの IP アドレスではなく IP アドレスのネットワーク部であるネットワークアドレスによって情報を保存している。これは、テーブルサイズの節約や経路制御の効率化のためである。IP は Internet 経路制御テーブルを利用するだけであり、このテーブルの更新には、RIP などのプロトコルが使われる。

そのほかの間接経路制御の方法としては、デフォルト経路、ホスト指定経路などがある。デフォルト経路は、ホストが 1 つのゲートウェイを介して Internet と繋がっているローカルネットワークに存在する場合を考えると理解しやすい。この場合、相手の IP アドレスのネットワーク部が自分の IP アドレスのそれと違っている場合はつねにデフォルト経路であるゲートウェイに IP データグラムを送ればよい。ホスト指定経路は、ネットワーク接続や経路制御テーブルなどのデバッグなどで利用される。

IP は IP データグラムの構造とその配送などについて定義された通信プロトコルである。したがって配送にともなって発生する問題を処理するようには定義されていない。経路制御の問題、ネットワークの障害、データグラムの輻輳などによる IP データグラムの配送の失敗などの報告のためのプロトコルが ICMP である。ホストではなくゲートウェイが実行するプロトコルであり、配送に失敗したゲートウェイからデータグラムの始点に ICMP メッセージを IP データグラムにカプセル化して送る。ICMP が扱う問題としては、到達不可能な終点の報告、輻輳とデータフロー制御、方向転換、循環と過長経路などがある。ICMP にはエラー報告のほかに、到達可能性テストの機能がある。この IMCP エコー要求、IMCP エコー応答を利用したプログラムに ping がある。

6 UDP と TCP

UDP と TCP は、ともに Internet 上のアプリケーションプログラム間の通信の機構を提供している。アプリケーションプログラムはポートという概念を通して UDP/TCP を利用する。アプリケーションから受け取ったデータはヘッダとデータから成る、UDP ではユーザデータグラム、TCP ではセグメントという単位にまとめて IP に送られる。

UDP は信頼性のない、コネクションレスな配送サービスを提供する。UDP の主要な機能はアプリケーションプログラムが IP を直接使用して IP データグラムを配送する方法を提供することである。UDP 自体には信頼性がないので、信頼性の確保は UDP を使用するアプリケーションプログラムに任されている。tftp などの単発で、オーバーヘッドの少ないデータグラム式の通信アプリケーションで使用される。

これまで述べてきたIPやUDPは信頼性のないサービスなのに対し、信頼性のある配送サービスを提供するのがTCPである。アプリケーションプログラムから見たTCPが提供する機能を要約すると以下のようになる。

- ストリーム指向
- バーチャルサーキットコネクション
- バッファ付き転送
- 非構造化ストリーム
- 全二重コネクション

バーチャルサーキットという言葉は、信頼性のない基盤の上に仮想的にアプリケーション間の専用の信頼性のある通信路を提供するという意味で使われている。

TCPセグメントのヘッダには、ポート番号、シーケンス番号、コードビットフィールドなどの制御情報が入っており、コードビットには、SYN、ACK、FINなどがある。TCPはアプリケーション間の通信サービスを提供するために、まずバーチャルサーキットを確保する。バーチャルサーキットのコネクションの確立や終了はSYN、ACK、FINなどをセットしたセグメントを利用して行なう。コネクションを確立した後は、シーケンス番号を利用してデータを順序づけている。

TCPで信頼性のない基盤を使って信頼性のある転送を提供している基本的ないくつかの技術について説明する。再転送付き肯定確認応答と呼ばれる技術は、送信したセグメントに対して受信側からの確認(コードビットのACK)の付いたセグメントが到着するまで次のセグメントを送信しないことを基本としている。同時に、送信時に再送タイマーをセットして時間内に確認が返らないと同じセグメントを再送する。しかしこの方法ではネットワークの距離による確認応答の遅延などによって通信路の帯域巾を浪費してしまい非効率である。そこでもう一つ、スライディングウィンドウという重要なアイディアが使われている。配送を待っているセグメント列の中に連続した複数のセグメントが入っているウィンドウを考える。このウィンドウ内のセグメントは確認応答に関係なく転送できることにする。転送したセグメントへの確認が返ってくると、確認のあったセグメントはウィンドウから外れ、新しいセグメントがウィンドウに入るようにスライドする。こうすることでウィンドウのサイズまでのセグメントは確認応答に関係なくネットワークの帯域巾を有効に利用して効率的な転送が可能になる。

セグメントの転送を開始する時点ではネットワークでの遅延は予測できない。これは転送する相手がどれくらい離れているか分からないためである。このため再送タイマーのタイムアウトの設定は確認応答の遅延を監視しながら補正していく必要がある。またスライディングウィンドウのサイズは、実際には、可変長になっておりネットワークの輻輳などに対応して変化させている。再送タイマやウィンドウサイズをネットワークやホストの状況に応じてダイナミックに変更することで効率的で信頼性のある転送を実現している。

7 おわりに

ここではTCP/IPプロトコルの基本的な部分について報告した。経路制御プロトコルを含むその他のプロトコルやクライアントサーバプログラミングなどについては省略した。今回の研修期間ではTCP/IPについて十分に理解するまでにはいかなかった。Internet、TCP/IPなどネットワークに関する技術は現在も大きく変化しており、これからもネットワーク技術について継続して理解を深めていきたいと思う。